Fact Sheet | Thursday, February 25, 2016

Apple's Motion to Vacate an Order Compelling Apple to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance

---

Apple has gone above and beyond what is required by law to support the government in its investigation. Within hours of being contacted, Apple produced information in its possession responsive to government inquiries and remained engaged with the government over the 6-week period as it conducted its investigation. Olle Dec. 6 -9

The Government is now asking that the court order Apple to do something that Congress has not authorized and that the DOJ and Executive branch expressly backed away from asking Congress to authorize, effectively hijacking an important national debate Br. 9

In order to comply with the Gov't demands, Apple would need to create a new "GovtOS" and FBI forensics lab on site that has the potential to be used on hundreds of phones now in law enforcements possession in conflict with existing law as well as the First and Fifth Amendment of the United States Constitution. EN Dec. 15-20, Olle Dec. 13 & 14, Br. 14, 32 and 34.

I. Today Apple filed a motion to vacate a California Magistrate Judge's February 16, 2016 order that would compel Apple to create software to allow FBI agents to hack into an iPhone 5c used in the San Bernadino attack.

   A. On February 16, 2016, without giving Apple notice or an opportunity to respond, the government asked the court to compel Apple to assist in the government's investigation under the authority of the All Writs Act of 1789. That same morning, the court granted the request and signed the government's proposed order. Brief at 12.

   B. The order requires Apple to write software creating "a backdoor to defeat the encryption on the iPhone, making its users' most confidential and personal information vulnerable to hackers, identity thieves, foreign agents, and unwarranted government surveillance." Brief at 1.

   C. No court has ever granted the government power to force companies like Apple to weaken its security systems to facilitate the government's access to private individuals' information. The All Writs Act does not support such sweeping use of judicial power, and the First and Fifth Amendments to the Constitution forbid it. Brief at 1.

II. The All Writs Act does not grant courts blanket authority "to change the substantive law, resolve policy disputes, or exercise new powers that Congress has not afforded them." Brief at 15.

A. "Congress has never authorized judges to compel innocent third parties to provide decryption services to the FBI." Brief at 15. In fact, Congress has expressly withheld this power in other contexts.

B. Congress has passed, and continues to create, laws that recognize the importance of privacy interests and law enforcement. Brief at 6–10. It would violate the separation-of-powers doctrine for the court to use the All Writs Act to expand the government's power beyond the authority afforded to it in these laws. Brief at 17–18.

C. "If anything, the question whether companies like Apple should be compelled to create a backdoor to their own operating systems to assist law enforcement is a political question, not a legal one." Brief at 18. The All Writs Act does not allow the government to short circuit the lawmaking process with a court order. Brief at 19.

III. The government's demand violates Apple's constitutional rights. Brief at 32–34.

A. The demand violates Apple's First Amendment rights against compelled speech and viewpoint discrimination. Apple wrote code for its operating system that reflects Apple's strong view about consumer security and privacy. By forcing Apple to write software that would undermine those values, the government seeks to compel Apple's speech and to force Apple to express the government's viewpoint on security and privacy instead of its own. Brief at 30–32.

B. The government's demand also violates Apple's Fifth Amendment right to be free from arbitrary deprivation of its liberties in that it would conscript Apple to develop software that undermines the security mechanisms of its own products. Brief at 34.